



PATENT ABSTRACTS OF JAPAN

(11) Publication number: 07154770 A

(43) Date of publication of application: 16 . 06 . 95

(51) Int. Cl

H04N 7/167

(21) Application number: 05326166

(71) Applicant: NEC CORP

(22) Date of filing: 30 . 11 . 93

(72) Inventor: OZAKI MITSURU

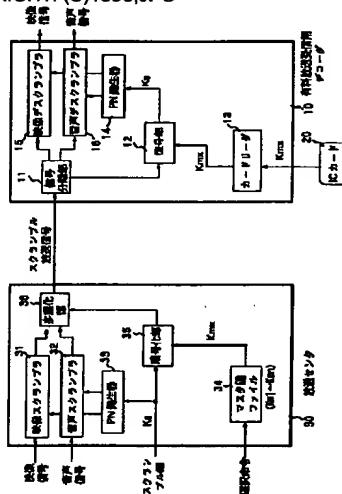
**(54) PAY TELEVISION BROADCAST
TRANSMISSION/RECEPTION SYSTEM AND
DECODER FOR RECEIVING PAY TELEVISION
BROADCAST**

(57) Abstract:

PURPOSE: To provide a pay television broadcast transmission/reception system and decoder capable of minimizing damage caused by illicit reception even when the state of illicit decoding the contents of a master key of one part is generated concerning the transmission/reception system for transmitting/receiving the pay television broadcast such as satellite broadcast or CATV and its decoder.

CONSTITUTION: A multiplex part 36 respectively multiplex a scramble key K_s , ciphered with a master key K_{mx} as a cryptographic key, to scrambled video and sound signals and transmits those signals. A decoder 10 for pay television broadcast reception reads the master key K_{mx} stored in an IC card 20 with a card reader 13 and decodes the scramble key K_s by inputting that master key to a decoding part 12 as a decode key. Since the master key K_s is changed periodically, it is necessary to newly purchase the IC card 20 periodically as well. The master key K_{mx} is used commonly for all the decoders.

COPYRIGHT: (C)1995,JPO



(51)Int.Cl.[®]

H 04 N 7/167

識別記号

庁内整理番号

F I

技術表示箇所

H 04 N 7/ 167

審査請求 有 請求項の数4 FD (全10頁)

(21)出願番号 特願平5-326166

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(22)出願日 平成5年(1993)11月30日

(72)発明者 尾崎 満

東京都港区芝5丁目7番1号 日本電気株式会社内

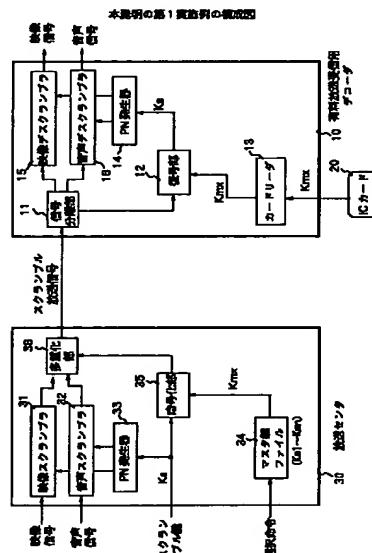
(74)代理人 弁理士 松浦 兼行

(54)【発明の名称】 有料放送送受信システム及び有料放送受信用デコーダ

(57)【要約】

【目的】 本発明は衛星放送やCATVなどの有料放送を送受信する送受信システム及び有料放送を受信するためのデコーダに関し、一部のマスタ鍵の内容が不正に解読される事態が発生しても不正受信による被害を最小限にし得る有料放送送受信システム及び有料放送受信用デコーダを提供することを目的とする。

【構成】 多重化部36はマスタ鍵K_mxを暗号鍵として暗号化されたスクランブル鍵K_sをスクランブル処理された映像信号及び音声信号にそれぞれ多重して送信する。有料放送受信用デコーダ10はICカード20に記憶されているマスタ鍵K_mxをカードリーダ13で読み取り、それを復号部12に復号鍵として入力し、スクランブル鍵K_sを復号させる。マスタ鍵K_sは一定期間毎に変更されるため、ICカード20も一定期間毎に新たに購入することが必要とされる。マスタ鍵K_mxは全デコーダに共通に用いられる。



【特許請求の範囲】

【請求項1】 擬似ランダム系列を用いて映像信号及び音声信号の少なくとも一方をスクランブル処理すると共に、該擬似ランダム系列の初期値を定めるスクランブル鍵を、マスタ鍵を暗号鍵とする暗号化処理をして前記少なくとも一方がスクランブル処理されている映像信号及び音声信号に多重し、該多重信号をスクランブル放送信号として送信し、

受信用デコーダでは、該スクランブル放送信号から前記映像信号及び音声信号と暗号化されたスクランブル鍵とをそれぞれ分離し、該暗号化されたスクランブル鍵を復号して擬似ランダム系列発生器の初期値を決定し、該擬似ランダム系列を用いて前記受信後分離した映像信号及び音声信号をデスクランブル処理する有料放送受信システムであって、

前記送信側において前記マスタ鍵として全受信用デコーダに共通のマスタ鍵を使用すると共に該マスタ鍵を一定期間毎に変更し、

前記受信用デコーダにおいては前記暗号化されたスクランブル鍵の復号鍵として用いるマスタ鍵を、外部から挿入される記録媒体から読み取り入力することを特徴とする有料放送受信システム。

【請求項2】 少なくとも一方がスクランブル処理されている映像信号及び音声信号と、全受信用デコーダ共通で、かつ、一定期間毎に変更されるマスタ鍵を暗号鍵として暗号化されたスクランブル鍵との多重信号であるスクランブル放送信号を受信し、少なくとも一方がスクランブル処理されている映像信号及び音声信号と、暗号化されたスクランブル鍵とをそれぞれ分離する信号分離部と、

外部より挿入される記録媒体からマスタ鍵を読み取る第1の読み取り手段と、

該第1の読み取り手段よりの該マスタ鍵を復号鍵として前記信号分離部から入力される暗号化されたスクランブル鍵を復号する復号部と、

該復号部よりのスクランブル鍵により初期値が設定される擬似ランダム系列発生器と、

該擬似ランダム系列発生器よりの擬似ランダム系列に基づいて前記信号分離部からのスクランブル処理されている映像信号及び/又は音声信号をデスクランブル処理するデスクランプルとを有することを特徴とする請求項1記載の有料放送受信システムに用いる有料放送受信用デコーダ。

【請求項3】 前記信号分離部により分離されるスクランブル放送信号中には前記スクランブル鍵と同じマスタ鍵により暗号化された課金種別情報が含まれており、外部より挿入される記録媒体からマスタ鍵と課金情報とを読み取り該マスタ鍵は前記復号部へ復号鍵として出する第2の読み取り手段と、

該第2の読み取り手段により読み取られた課金情報と、

前記信号分離部より入力される前記課金種別情報とが入力され、該課金情報に基づいて前記擬似ランダム系列発生器へ動作許可の有無を示す信号を出力すると共に、該課金種別情報に基づいて所定の課金種別のときに新しい残度数を算出する課金制御部と、

該課金制御部により算出された新しい残度数を前記記録媒体に更新記録する記録手段と、前記第1の読み取り手段に代えて設けたことを特徴とする請求項2記載の有料放送受信用デコーダ。

【請求項4】 前記記録媒体はICカードであり、前記擬似ランダム系列発生器はPN系列を発生することを特徴とする請求項2又は3記載の有料放送受信用デコーダ。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は有料放送受信システム及び有料放送受信用デコーダに係り、特に衛星放送やケーブルテレビジョン(CATV)などの有料放送を送受信する送受信システム及び有料放送を受信するためのデコーダに関する。

【0002】 衛星放送やCATVなどの有料放送では、不正受信防止のため、放送センタにおいて映像信号及び/又は音声信号(以下、「放送信号」という)を、電気的に攪拌するスクランブル処理をしてから送信することが一般的に行われる。この放送信号を受信し、正常に再生するためには、放送センタでスクランブルを動作させるに使用したスクランブル鍵を手に入れ、このスクランブル鍵を用いて有料放送受信用デコーダ内のデスクランブルを動作させればよい。

【0003】 スクランブル鍵は通常、データ信号と混合された後、放送信号に多重化されて各受信者宅に設置されたデコーダまで配布される。従って、有料放送放送企業と正規に契約していない者が何らかの手段によりスクランブル鍵を手に入れた場合には、契約者以外の者でも容易に有料放送を不正に受信できてしまう。このため、スクランブル鍵が不正に解読されたとしても、不正受信を最小限に止める有料放送受信用デコーダが必要とされる。

【0004】

【従来の技術】 図3は文献(平成2年度の電気通信技術審議会答申諮問第44号76頁)に開示されている、従来の有料放送受信システムの一例の構成図を示す。同図において、30は放送センタ、40は従来の有料放送受信用デコーダを示す。放送センタ30は、映像スクランブル31、音声スクランブル32、PN発生器33、多重化部36、受信者別マスタ鍵ファイル37、暗号化部38及び39よりなる。また、有料放送受信用デコーダ40は、信号分離部41、PN発生器44、映像デスクランブル45、音声デスクランブル46、マスタ鍵記憶部41、復号部42、43、及び契約条件比較回路4

4よりなる。

【0005】放送センタ30においては、PN発生器3の初期値がスクランブル鍵Ksにより設定され、このPN発生器3より出力されるPN系列（擬似ランダム系列）を映像スクランブル31及び音声スクランブル32にそれぞれ入力して、放送する映像信号と音声信号に別々にスクランブル処理を行う。上記のスクランブル鍵Ksは第三者に知られないようにするために、放送局識別情報やサービスなどの共通情報と共に暗号化部39により暗号化される。

【0006】ここで、スクランブル鍵Ksの伝送時の暗号鍵としてワーク鍵Kwが暗号化部39に入力される。また、契約内容やデコーダIDなどの個別情報は受信者別マスタ鍵ファイル37に入力されて、受信者毎（デコーダ毎）に異なるマスタ鍵Kmiが読み出される。このマスタ鍵Kmiは暗号化部38に暗号鍵として入力され、前記ワーク鍵Kw及び個別情報の暗号化部38での暗号に用いられる。

【0007】映像スクランブル31、音声スクランブル32、暗号化部38及び39の各出力信号は多重化部36に入力されて多重された後、スクランブル放送信号として各受信者に送信される。スクランブル鍵Ksは送信、受信のPN発生器33、34の同期のために送信される。

【0008】有料放送受信用デコーダ40は上記のスクランブル放送信号を受信し、多重化部36においてそれぞれ多重された各信号を信号分離部11にて分離する。これにより、スクランブルされた映像信号は映像デスクランブル15に入力され、スクランブルされた音声信号は音声デスクランブル16に入力され、暗号化部38の出力暗号信号は復号部42に入力され、更に暗号化部39の出力暗号信号は復号部43に入力される。

【0009】デコーダ40は固有のマスタ鍵Kmiを記憶している記憶部41を有しており、このマスタ鍵Kmiを用いて復号部42により復号動作を行わせ、受信したスクランブル放送信号中のワーク鍵Km及び個別情報を復号する。復号されたワーク鍵Kwは復号部43に復号鍵として入力され、ここで受信したスクランブル放送信号中のスクランブル鍵Ks及び共通情報をそれぞれ復号させる。

【0010】復号部42より取り出された個別情報及び復号部43より取り出された共通情報は、それぞれ契約条件比較回路44に入力され、ここで所定の契約条件を満足するか否か自動的に判定される。契約条件を満足するときには契約条件比較回路44からPN発生器14へ作動信号が出力される。このPN発生器14は作動信号が入力され、かつ、復号部43より正しいスクランブル鍵Ksが入力されたときに、放送センタ30内のPN発生器33より出力されるPN系列と同じPN系列を発生し、映像デスクランブル15及び音声デスクランブル1

6にそれぞれ入力する。

【0011】このようにして、映像デスクランブル15からはスクランブル処理が解除された映像信号が取り出され、また音声デスクランブル16からはスクランブル処理が解除された音声信号が取り出される。

【0012】なお、従来の有料放送受信用デコーダには、契約条件比較回路44での契約条件比較を外部からのカードから読み取った課金条件なども含めて比較するものも知られている（例えば、特開平2-111185号公報）。

【0013】

【発明が解決しようとする課題】従来の有料放送受信用デコーダ40においては、デコーダ毎に設定された復号用マスタ鍵Kmi（ここでiはデコーダ毎に付与されたID番号）は、ICチップの形態でデコーダ40内に41で示す如く組み込まれており、容易に取り外しができない構造とされている。

【0014】しかしながら、図3に示した従来の有料放送受信用デコーダや、カードにより課金条件を入力するような従来の有料放送用デコーダでは、マスタ鍵Kmiはデコーダ内にハードウェアの形態で内蔵されているため、ひとたびマスタ鍵Kmiの内容が不正に解読された場合には、ワーク鍵Kw及びスクランブル鍵Ksがそれぞれ復号されてしまい、これに対抗する手段がない。唯一、放送センタ側のマスタ鍵ファイル37中の該当するマスタ鍵Kmiを変更すれば対抗することができるが、どのマスタ鍵が解読されたかを知る方法がないことから事実上該当するマスタ鍵Kmiだけを変更することは不可能である。また、マスタ鍵ファイル37の内容を全面的に変更するのでは、正規にデコーダを購入して所有している受信者が受信できなくなってしまう。

【0015】また、放送センタ30側では、各デコーダで異なるマスタ鍵情報のうち料金滞納者や契約終了者などの分を除いた正規加入者分のすべてのマスタ鍵を送出しなければならず、このため加入者数が増えれば増えるほど煩雑で時間のかかる作業を行う必要がある。

【0016】本発明は以上の点に鑑みなされたもので、一定期間毎にマスタ鍵の内容を変更することにより、一部のマスタ鍵の内容が不正に解読される事態が発生しても不正受信による被害を最小限にし得る有料放送受信システム及び有料放送受信用デコーダを提供することを目的とする。

【0017】

【課題を解決するための手段】上記の目的を達成するため、本発明の有料放送受信システムは擬似ランダム系列を用いて映像信号及び音声信号の少なくとも一方をスクランブル処理すると共に、擬似ランダム系列の初期値を定めるスクランブル鍵を、マスタ鍵を暗号鍵とする暗号化処理をして前記映像信号及び音声信号に多重してスクランブル放送信号として送信し、受信用デコーダで

は、スクランブル放送信号から前記映像信号及び音声信号と暗号化されたスクランブル鍵とをそれぞれ分離し、暗号化されたスクランブル鍵を復号して擬似ランダム系列発生器の初期値を決定し、擬似ランダム系列を用いて前記受信後分離した映像信号及び音声信号をデスクランブル処理する有料放送受信システムであって、送信側において前記マスタ鍵として全受信用デコーダに共通のマスタ鍵を使用すると共にマスタ鍵を一定期間毎に変更し、受信用デコーダにおいては前記暗号化されたスクランブル鍵の復号のための復号鍵として用いるマスタ鍵を、外部から挿入される記録媒体から読み取り入力する構成としたものである。

【0018】また、本発明の有料放送受信用デコーダでは、前記スクランブル放送信号を受信し、少なくとも一方がスクランブル処理されている映像信号及び音声信号と、暗号化されたスクランブル鍵とをそれぞれ分離する信号分離部と、外部より挿入される記録媒体からマスタ鍵を読み取る第1の読み取り手段と、第1の読み取り手段よりのマスタ鍵を復号鍵として信号分離部から入力される暗号化されたスクランブル鍵を復号する復号部と、復号部よりのスクランブル鍵により初期値が設定される擬似ランダム系列発生器と、擬似ランダム系列に基づいて信号分離部からのスクランブル処理されている映像信号及び/又は音声信号をデスクランブル処理するデスクランプラとを有する構成としたものである。

【0019】更に、請求項3記載の有料放送受信用デコーダでは、外部より挿入される記録媒体からマスタ鍵と課金情報を読み取りマスタ鍵は復号部へ復号鍵として出力する第2の読み取り手段と、この課金情報と信号分離部より入力される課金種別情報とが入力され、課金情報に基づいて擬似ランダム系列発生器へ動作許可の有無を示す信号を出力すると共に、課金種別情報に基づいて所定の課金種別のときに新しい残度数を算出する課金制御部と、この新しい残度数を記録媒体に更新記録する記録手段とを、前記請求項2記載の有料放送受信用デコーダの第1の読み取り手段に代えて設けた構成としたものである。

【0020】

【作用】本発明の有料放送受信システムでは、送信スクランブル放送信号中のマスタ鍵を一定期間毎に変更するようにしているため、外部からデコーダに挿入される記録媒体も送信スクランブル放送信号中のマスタ鍵に対応して一定期間毎に同じマスタ鍵が記録された記録媒体に変更するようにさせることができる。

【0021】また、請求項2記載の有料放送受信用デコーダでは、第1の読み取り手段により、外部から挿入される記録媒体から読み取るマスタ鍵は、受信者対応のものではなく、すべての受信者（すべてのデコーダ）に共通の同一のマスタ鍵であるため、有料放送受信用デコーダをすべての受信者に共通の構成とすることができます。

また、外部から記録媒体を挿入するだけで有料放送を受信することができる。

【0022】更に、請求項3記載の有料放送受信用デコーダでは、課金種別が所定の種別のときには、課金制御部により新しい残度数を算出し、その残度数を記録手段により記録媒体に更新記録するようによっているため、送信側では残度数を管理する必要がなく、記録媒体に記録されている常に最新の残度数に基づく有料放送受信ができる。

10 【0023】

【実施例】次に、本発明の実施例について説明する。図1は本発明の第1実施例の構成図を示す。同図中、図3と同一構成部分には同一符号を付してある。図1において、10は本発明の有料放送受信用デコーダの第1実施例で、信号分離部11、復号部12、カードリーダ13、PN発生器14、映像デスクランプラ15及び音声デスクランプラ16より構成されている。

【0024】カードリーダ13はICカード20の記録情報を読み取る機器で、前記第1の読み取り手段を構成している。また、ICカード20は受信しようとするスクランブル放送信号中の暗号化されているスクランブル鍵K_sを復号するための復号鍵となるマスタ鍵K_m xが記録されている記録媒体である。PN発生器14は擬似ランダム系列であるPN系列を発生する回路で、その初期値はスクランブル鍵K_sにより設定される。

【0025】30は放送センタで、有料放送受信用デコーダ10と共に有料放送受信システムを構成している。放送センタ30は映像スクランプラ31、音声スクランプラ32、PN発生器33、マスタ鍵ファイル34、暗号化部35及び多直化部36より構成されている。PN発生器33はPN発生器14と同一構成の擬似ランダム系列発生器である。また、マスタ鍵ファイル34は多数のマスタ鍵K_m 1～K_m nを収納しており、外部からの選択命令によりそのうちのひとつマスタ鍵K_m xが選択される。このマスタ鍵K_m xは一定期間毎（例えば6ヶ月毎）に変更されるようになされている。

【0026】ところで、有料放送の契約内容としては、チャンネル毎に月極めで定額料金を支払うことによりそのチャンネルのすべての番組を視聴することができるフ

40 ラットフィー、いくつかの番組及び料金設定方式を組み合わせた番組表や料金一覧表を用意し、この中から視聴者が選択して契約するティア、個別番組毎に料金を設定し、視聴した番組だけに課金するペイパー・プログラム、単位時間毎に所定の料金が設定されており、視聴した時間分に課金するペイパー・タイムなどがある。本実施例は、このうち、フラットフィー方式の有料放送に有効なシステムである。

【0027】次に、本実施例の動作について説明する。まず、放送しようとする映像信号及び音声信号はそれぞれ対応する映像スクランプラ31及び音声スクランプラ

32に入力され、ここでPN発生器33より供給されるPN系列に基づきスクランブル処理が行われる。スクランブル処理の具体的方法は種々提案されている(例えば映像信号に関しては走査線内信号切替方式、走査線転移方式、あるいはこれらの併用方式など、また音声信号に関してはPN信号系列加算方式など)が、これらは公知であり、また本発明の要旨ではないのでその詳細な説明は省略する。

【0028】上記の映像スクランブル31及び音声スクランブル32におけるスクランブルに用いられるPN系列の初期値は、スクランブル鍵Ksにより設定される。このスクランブル鍵Ksは暗号化部35に入力され、ここでマスク鍵ファイル34から選択命令に従って読み出されたマスク鍵Kmxを暗号鍵として暗号化される。マスク鍵Kmxはすべての受信用デコーダに共通に用いられ、また、前記したように一定期間毎に変更される。

【0029】暗号化されたスクランブル鍵Kmxと映像スクランブル31及び音声スクランブル32よりそれぞれスクランブル処理されて取り出された映像信号及び音声信号とは多重化部36において多重化される。この多重化部36より取り出された多重信号はスクランブル放送信号として無線又は有線にて送信される。

【0030】有料放送受信希望者(加入者)は、有料放送放送局(又はその代行者)から有料放送受信用デコーダ10とICカード20とを料金前払いにて購入する。ICカード20にはマスク鍵情報(ここではKmx)が予め記録されている。このICカード20は有料放送受信用デコーダ10内に挿入されることにより、カードリーダ13でその記録情報が読み取られ、そのうちマスク鍵Kmxが復号部12に復号鍵として入力される。

【0031】一方、有料受信用デコーダ10はスクランブル放送信号を受信し、信号分離部11により受信信号からスクランブル処理されている映像信号と、スクランブル処理されている音声信号とをそれぞれ分離して映像デスクランブル15及び音声デスクランブル16にそれぞれ入力すると共に、受信信号から暗号化されているスクランブル鍵Ksを分離して復号部12に入力する。

【0032】復号部12はこの暗号化されているスクランブル鍵Ksを、カードリーダ13からのマスク鍵Kmxを復号鍵として復号し、放送センタ30において用いられたスクランブル鍵Ksを復号する。復号されたスクランブル鍵KsはPN発生器14に入力されてその出力PN系列の初期値を定める。

【0033】これにより、PN発生器14からは放送センタ30より出力されたPN系列と同期したPN系列が取り出され、映像デスクランブル15及び音声デスクランブル16にそれぞれ供給されてデスクランブル処理を行わせる。その結果、映像デスクランブル15及び音声デスクランブル16からは、それぞれスクランブルが解除された正常な映像信号及び音声信号が取り出される。

【0034】本実施例では、マスク鍵Kmxは一定期間後に別の値のマスク鍵(例えばKmy)に変更される。このため、マスク鍵Kmxの情報が記録されているICカード20を用いても有料放送を受信することができなくなる。そこで、受信希望者は新しいマスク鍵Kmyの情報が記録されている別のICカードを新たに購入して、これを有料放送受信用デコーダ10に挿入することにより、再び受信することができる。

【0035】従って、何らかの手段によりスクランブル鍵Ksあるいはマスク鍵Kmxが不正に解読されたときには、従来では何らの対抗手段もなかったが、本実施例によれば、最長でも上記の一定期間のみしか不正視聴ができないため、不正視聴による被害を最小限に止めることができる。

【0036】また、本実施例ではマスク鍵Kmxなどはすべての有料放送受信用デコーダ10に共通であるため、有料放送受信用デコーダ10はすべて同一構成とすることができるため、デコーダ製造コストを従来よりも安価にすることができる、更に従来の放送センタでの受信者対応のマスク鍵ファイル作成作業の煩雑さを除去することができる。また、本実施例では、有料放送受信用デコーダ10を動作させるためにはICカード20を料金前払いにて購入する必要があるため、従来生じていた長期滞納者に対する送信停止前の既放送分の料金の未回収を防止することができる。

【0037】次に、本発明の第2実施例について説明する。図2は本発明の第2実施例の構成図を示す。同図中、図1と同一構成部分には同一符号を付し、その説明を省略する。図2において、10'は本発明の有料放送受信用デコーダの第2実施例で、第1実施例のカードリーダ13に代えて、カードリーダ/ライタ18及び課金制御部19が設けられている点に特徴がある。

【0038】カードリーダ/ライタ18はICカードの記録情報を読み取る機能と、ICカードに入力情報を受け取る機能とをそれぞれ有する機器で、前記した第2の読み取り手段及び記録手段とを構成している。また、放送センタ30内の暗号化部35'はスクランブル鍵Ksと共に課金種別情報も併せて暗号化する構成とされている。本実施例はペイパービュー(すなわち、ペイパープログラム及びペイバータイム)に有効な有料放送受信システムである。

【0039】次に、本実施例の動作について説明する。放送センタ30では、暗号化部35'において、スクランブル鍵Ksと共に放送番組がフラットキーであるかペイパービュー(すなわち、ペイパープログラム及びペイバータイム)であるかを示す課金種別情報が、マスク鍵ファイル34からのマスク鍵Kmxを暗号鍵として暗号化される。

【0040】この暗号化部35'で暗号化されたスクランブル鍵Ks及び課金種別情報は、多重化部36において

て映像スクランブル31及び音声スクランブル32よりそれぞれスクランブル処理されて取り出された映像信号及び音声信号と多重化されてスクランブル放送信号とされて無線又は有線にて送信される。

【0041】有料放送受信希望者(加入者)は、有料放送放送局(又はその代行者)から有料放送受信用デコーダ10¹とICカード21とを料金前払いにて購入する。ICカード21にはマスタ鍵情報(ここではKm x)と共に、その受信希望者の残度数を示す課金情報が予め記録されている。このICカード21は有料放送受信用デコーダ10¹内に挿入されることにより、カードリーダ/ライタ18でその記録情報が読み取られ、そのうちマスタ鍵Km xが復号部12に復号鍵として入力され、課金情報が課金制御部19へ入力される。

【0042】一方、有料放送受信用デコーダ10¹は放送センタ30から送信されたスクランブル放送信号を受信し、信号分離部11により受信信号からスクランブル処理されている映像信号と、スクランブル処理されている音声信号とをそれぞれ分離して映像デスクランブル15及び音声デスクランブル16にそれぞれ入力するとと共に、受信信号から暗号化されているスクランブル鍵Ksと課金種別情報を分離して復号部12に入力する。

【0043】課金制御部19はカードリーダ/ライタ18より入力されるICカード21に記録されていた課金情報に基づいて残度数を調べ、残度数がゼロでないときに限り、PN発生器14に動作許可信号(命令)を送出する。PN発生器14はこの動作許可信号が入力されている場合に限り、復号化部12からのスクランブル鍵Ksに基づくPN系列を発生して映像デスクランブル15及び音声デスクランブル16にそれぞれ供給し、それぞれスクランブル処理が解除された映像信号及び音声信号を出力させる。

【0044】また、課金制御部19は復号部12から入力される前記課金種別情報に基づき、現在受信中の番組がフラットフィーであるかペイパービューであるかを識別し、受信中は有料放送受信用デコーダ10¹内に挿入された状態で保持されているICカード21に対して、ペイパービューと識別した場合に限り、ペイパーブログラムかペイパータイムかの種類に応じて規定料金を算出し、その算出した規定料金分の度数をICカード21の残度数から減じて新しい残度数を書き込む動作を繰り返す。

【0045】本実施例も第1実施例と同様に、マスタ鍵Km xは一定期間後に別の値のマスタ鍵(例えばKm y)に変更される。このため、マスタ鍵Km xの情報が記録されているICカード21を用いても有料放送を受信することができなくなる。そこで、受信希望者は新しいマスタ鍵Km yの情報と課金種別情報とが記録されている別のICカードを新たに購入して、これを有料放送受信用デコーダ10¹に挿入することにより、再び受信

することができる。

【0046】従って、本実施例も何らかの手段によりスクランブル鍵Ksあるいはマスタ鍵Km xが不正に解読されたときでも、不正視聴による被害を最小限に止めることができるなどの第1実施例と同様の特長を有すると共に、それに加えてICカード21の残度数を更新記録するようにしているため、課金を確実に行えるという特長がある。

【0047】なお、本発明は以上の実施例に限定されるものではなく、例えばマスタ鍵Km xや課金情報を記録する記録媒体はICカード以外の磁気カード、コンパクトディスク、磁気ディスクその他の記録媒体でもよく、またマスタ鍵ファイル34の代わりに選択指令に応じて所望のマスタ鍵を自動生成する回路を用いることにより、記憶容量の制限をなくすようにしてもよい。また、本発明は映像信号及び音声信号のどちらか一方のみに対してスクランブル処理を行う有料放送受信システムにも適用することができることは勿論である。

【0048】

【発明の効果】以上説明したように、本発明の有料放送受信システムによれば、デコーダを動作させるために必要な外部からデコーダに挿入される記録媒体を、スクランブル放送信号中のマスタ鍵に対応して一定期間毎に同じマスタ鍵が記録された記録媒体に変更しなければならないようにしたため、何らかの手段によりスクランブル鍵あるいはマスタ鍵が不正に解読されたときでも、従来に比べてデコーダの構造を複雑にすることなく、不正視聴による被害を最小限に止めることができ、また、従来の放送センタでの受信者対応のマスタ鍵ファイル作成作業の煩雑さを除去することができる。

【0049】また、本発明の有料放送受信用デコーダによれば、すべての受信者(すべてのデコーダ)に共通の同一のマスタ鍵が記録された記録媒体を使用することにより、有料放送受信用デコーダをすべての受信者に共通の構成とすることができるようにならため、デコーダ製造コストを従来よりも安価にことができる。

【0050】更に、本発明の有料放送受信用デコーダによれば、課金種別が所定の種別のときには、課金制御部により新しい残度数を算出し、その残度数を記録手段により記録媒体に更新記録することにより、送信側では残度数を管理する必要がなく、記録媒体に記録されている常に最新の残度数に基づく有料放送受信ができるようにならため、課金が確実にできる。

【図面の簡単な説明】

【図1】本発明の第1実施例の構成図である。

【図2】本発明の第2実施例の構成図である。

【図3】従来の有料放送受信システムの一例の構成図である。

【符号の説明】

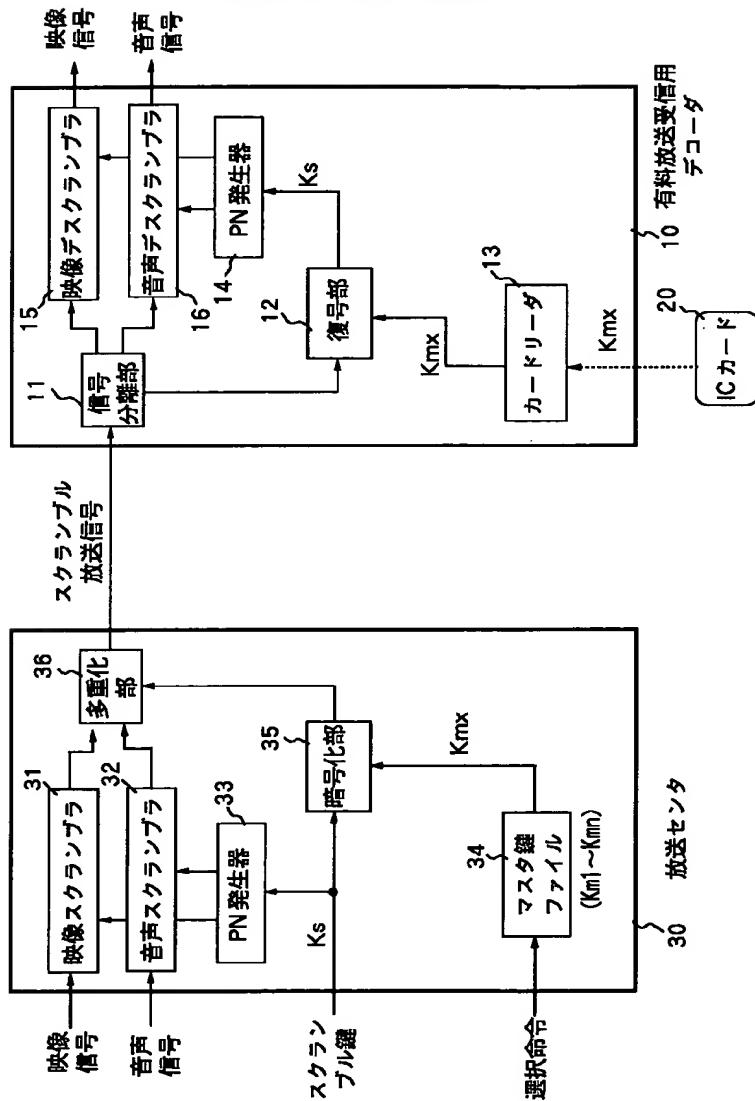
10, 10¹ 有料放送受信用デコーダ

- 1 1 信号分離部
- 1 2 復号部
- 1 3 カードリーダ
- 1 4、3 3 P N発生器
- 1 5 映像デスクランプラ
- 1 6 音声デスクランプラ

- * 1 8 カードリーダ／ライタ
- 1 9 課金制御部
- 2 0、2 1 I Cカード
- 3 0 放送センタ
- 3 4 マスク鍵ファイル
- * 3 5、3 5' 暗号化部

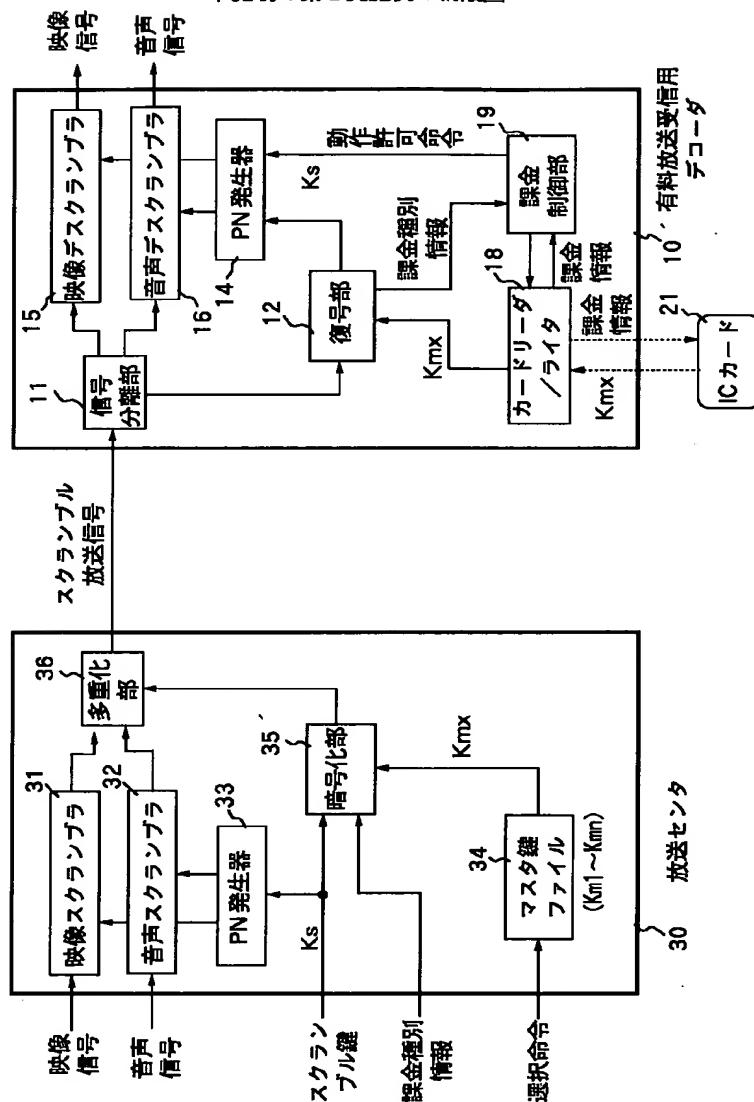
【図1】

本発明の第1実施例の構成図



【図2】

本発明の第2実施例の構成図



【図3】

